Status:	**Active Policy**
Effective Date:	September 24, 2007 through September 23, 2009
Revised Date:	N/A
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-103; UCA §63F-1-206; Utah Administrative Code, R895-7 Acceptable Use of Information Technology Resources; Utah Administrative Code, R477-11 Discipline*

1701.1 PURPOSE

This policy defines and establishes a security policy relating to the handling of confidential information which is under the custodial care of the State of Utah.

1701.1.1 Background

On December 11, 2001, the Governor of Utah issued an executive order directing the Chief Information Officer (CIO) to develop and implement policies that promote the security of state information and information systems. The CIO has determined that information security is an issue for all state agencies, and the Department of Technology Services (DTS) will assist agencies to govern and protect their information assets.

DTS will develop and implement security controls based on business rules which govern access and provide sufficient protection for each information asset. DTS will safeguard information assets through the application and enforcement of special precautions in the handling of confidential information that has been entrusted to its custodial care.

1701.1.2 Scope

This policy applies to all employees and contractors within the Department of Technology Service. State agencies and administrative subunits of state government, as defined by UCA §63F-1-102(7), et seq., are encouraged to abide by the provisions of this policy.

1701.1.3 Exceptions

The CIO may grant a policy exception when the requesting agency's Executive Director/Commissioner, or their designee, and the CIO determine that compliance would be overly burdensome and/or detrimental to the mission of the state. All exceptions must be approved in writing by the CIO.

1701.2 DEFINITIONS

Agency Security Officer
An employee assigned by the director or commissioner to coordinate and assist with the implementation and management of information security and security services for an Executive Branch Agency.

Authorized Information Users
Individuals, including employees, vendors, and visitors, who are given permission (authorized) to access State Information Assets.

Confidential Information
For the purposes of this policy Confidential Information include, but are not limited to, financial, health, social-security, criminal, biometric, or any other personally identifiable information which, if inappropriately disclosed, could lead to a significant negative impact on the subject. Confidential Information may also include information designated as confidential, private, controlled or any other equivalent term within statute, rule, policy or regulation.

Executive Branch Agency
For the purposes of this policy an Executive Branch Agency is an agency or administrative subunit of state government as defined by UCA §63F-1-102(7), et seq.

Information Technology Asset
For the purposes of this policy Information Technology Assets include, but are not limited to, hardware, software, and data owned, leased, rented, operated, controlled, assigned to or maintained by an Executive Branch Agency. Information Technology Assets may also include licenses, training programs and materials, maintenance agreements, and support services owned, leased, rented, operated, controlled, assigned to or maintained by an Executive Branch Agency.

State Information Asset
For the purposes of this policy State Information Asset include, but is not limited to, any unit of data which is prepared, owned, received, or retained by a governmental entity that in its original form is reproducible by mechanical or electronic means.

Vulnerability Mitigation
The process of addressing vulnerabilities such that the risks posed by such vulnerabilities are removed or reduced to acceptable levels. Examples include anti-virus tools, anti-spyware tools, patch management, and manual configuration changes.

1701.3 POLICY

The State of Utah is responsible for the security of all confidential information under its custodial care. In addition to any requirements set forth by statute or regulation, the agencies and administrative subunits of the State of Utah must, at a minimum, secure confidential information using the following guidelines:

1701.3.1 Information technology networks are to be adequately segmented and filtered to limit traffic to explicitly authorized and necessary connections.

1701.3.2 All assets are to be properly configured and maintained. This includes using secure, documented configurations and vulnerability mitigation.

1701.3.3 Custom information technology applications are to be written using secure development guidelines and best practices.

1701.3.4 Access to assets or confidential information is to be limited to authorized individuals with a need-to-know. A unique network identification will be assigned to all authorized individuals and the activities of each individual must be maintained in an audit record at all times.

1701.3.5 All confidential information assets are to be monitored for suspicious activity.

1701.3.6 All assets are to undergo regular risk assessments, including vulnerability scans and penetration tests.

1701.3.7 The Agency Security Officer will immediately notify the Enterprise Information Security Office (EISO) of any suspicious activity, breech of security, or loss of confidential information so that the incident can be handled according to established incident response policy and procedures.

1701.4 POLICY COMPLIANCE

The CIO may monitor compliance of this policy within the State Executive Branch, and report any findings or violations of this policy to an agency's Executive Director or designee. A State Executive Branch agency's Executive Director, or designee, upon becoming aware of a violation of this policy shall provide the CIO a report of action(s) taken in response to violation of this policy.

DOCUMENT HISTORY

Originator:	Michael Casey, Chief Information Security Officer
Next Review:	August 10, 2009
Reviewed Date:	N/A
Reviewed By:	N/A